

UNITED STATES DISTRICT COURT  
for the  
Eastern District of Wisconsin

In the Matter of the Search of:

Information associated with Facebook user ID 506758797  
and 511640886, that is stored at the premises controlled by  
Facebook

Case No. 17-M-141

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property:

See Attachment A.

located in the Eastern District of Wisconsin, there is now concealed:

See Attachment B.

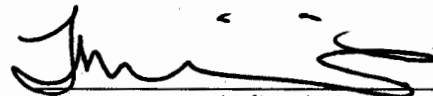
The basis for the search under Fed. R. Crim P. 41(c) is:

- ☒ evidence of a crime;  
☐ contraband, fruits of crime, or other items illegally possessed;  
☐ property designed for use, intended for use, or used in committing a crime;  
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to violations of: Bank Fraud, Title 18, United States Code, Section 1344; and Aggravated Identity Theft, Title 18, United States Code, Section 1028A

The application is based on these facts: See attached affidavit.


☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

  
Applicant's signature

United States Postal Inspector Theresa R. Williams  
Printed Name and Title

Sworn to before me and signed in my presence:

Date: Sept. 20, 2017

  
Judge's signature

City and State: Milwaukee, Wisconsin 00141-DEJ Filed 12/07/18 Page 1 of 32 Document 1  
Honorable David E. Jones U.S. Magistrate Judge  
Printed Name and Title

**AFFIDAVIT IN SUPPORT OF  
AN APPLICATION FOR A SEARCH WARRANT**

I, Theresa R. Williams, being duly sworn under oath, state as follows:

**I. INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of an application for a search warrant for information associated with certain Facebook accounts that are stored at premises owned, maintained, controlled, or operated by Facebook, a social networking company headquartered in Menlo Park, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. § 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Facebook to disclose to the government records and other information in its possession, pertaining to the subscribers or customers associated with the specified Facebook accounts.

2. I am currently employed as a United States Postal Inspector, assigned to the Milwaukee, WI office of the United States Postal Inspection Service (USPIS). I am a sworn federal law enforcement officer, empowered to investigate criminal activity involving or relating to the United States Postal Service (USPS) and/or United States Mail. In addition to the training and experience that I have obtained as a United States Postal Inspector, I have training as a Chicago Police Officer and, before joining the USPIS, had over fifteen years of training and experience as an accountant investigating and analyzing financial information. I am currently assigned to a multi-functional team which investigates crimes including, but not limited to, identity theft, mail theft, mail fraud, transportation of controlled substances or proceeds through the United States mail, and other crimes against or involving the United States mail. This affidavit is in support of an ongoing investigation into a scheme that involves utilizing the United States mails to transfer, possess, or use, without lawful authority, the identification of another person.

3. The information contained in this affidavit is either the result of personal observations and investigation, the review of law enforcement files or records, postal records, or is information that has been relayed to me by other law enforcement agents or citizen witnesses, all of whom I believe to be reliable. This affidavit is also based upon information gathered from interviews of witnesses and victims, reports, official records, law enforcement reports, and my training and experience.

4. More specifically, I seek authorization to search Facebook's information associated with the following individuals, also included in Attachment A, whom I have identified by their name as well as how their respective accounts are identified by Facebook:

| NAME           | FACEBOOK IDENTIFICATION (UID) | FACEBOOK NAME     |
|----------------|-------------------------------|-------------------|
| Anthony Sykes  | 506758797                     | Anthony.y.sykes   |
| Deandre Miller | 511640886                     | Deandremiller1987 |

5. The information I seek is stored at premises owned, maintained, controlled, or operated by Facebook, a social networking company headquartered in Menlo Park, California, from at least approximately July 1, 2013 to November 1, 2013.

6. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of Title 18 U.S. Code § 1344 – Bank Fraud and 18 U.S. Code § 1028A - Aggravated identity theft, have been committed by Edward Anthony Williams, Anthony Sykes, and Deandre Miller. There is also probable cause to search the information described in Attachment A for evidence of these crimes, as described in Attachment B. Since this affidavit is only for the limited purpose of securing a search warrant, I have not set forth each and every fact known to me concerning this investigation. I have included what I believe are facts sufficient to establish probable cause for the warrants sought.

## **II. CASE SUMMARY**

7. In August 2013, and continuing through October 2013, Edward Williams, Anthony Sykes, and Deandre Miller conspired to defraud US Bank in Milwaukee, WI. Sykes, an Illinois native, provided personal identity information to Williams to fraudulently open three separate accounts at US Bank using stolen identities. US Bank checking accounts, savings accounts, and lines of credit were created for all three fraudulently created accounts and debit cards and credit cards were issued on the accounts. The bank statements, credit cards and debit cards were all mailed to three different addresses in and around Chicago, IL, linked to both Miller and Sykes. The credit and debit cards were subsequently used to make purchases and withdraw money from the accounts as described below. In all, the fraudulent transactions executed on the credit and debit cards resulted in a potential loss of \$35,744.35, and an actual loss of \$23,795 to US Bank, a financial institution insured by the FDIC at the time the offenses occurred.

8. During the fraud, Williams worked as an assistant manager at the US Bank in store branch at the Walmart located at 10330 W. Silver Spring Drive in Milwaukee, WI. Williams fraudulently opened three US Bank accounts while other subjects involved in the conspiracy came into the bank branch to pose as the account holder. As Williams, Sykes and Miller well knew, however, none of the three accounts involved were opened by the named account holders. Typically, the defendants opened the accounts with a very small deposit totaling no more than \$25. The checking accounts were linked to a line of credit totaling approximately \$2,500 to \$5,000. After opening the accounts, the line of credit was immediately accessed, and those funds were deposited into the checking account. Money was then withdrawn from the accounts through ATM withdrawals and debit purchases. At the same time, the defendants also had US Bank issued credit cards with credit limits ranging from \$5,000 to \$17,000. Purchases were made using the credit

cards, and cash advances were pulled from the credit card accounts and deposited into the checking accounts. Money was then withdrawn from the accounts through ATM withdrawals and debit purchases. The accounts were open for short periods of time, typically less than two months. At least one minimum payment on each account was made to keep the accounts active. Numerous individuals were photographed making withdrawals from the three accounts at ATM's primarily in Illinois, but also in Wisconsin.

9. In October 2013, Williams was confronted by US Bank fraud investigators and admitted to his participation in fraudulently opening the three accounts. Williams also later identified both Sykes and Miller as participants.

10. Bank statements for the accounts reflect that illegal purchases and ATM transactions on the three accounts occurred in and around Milwaukee, WI, Chicago, IL, and Baltimore, MD. On September 5, 2017, several transactions were traced back to Sykes and Miller after evidence of the illegal transactions were located on their Facebook page. The offense conduct and Facebook activity of the subjects is discussed in detail below.

### **III. PROBABLE CAUSE**

11. On August 6, 2013, a checking account, savings account, and line of credit and were opened by Assistant Manager Edward Anthony (Tony) Williams at the U.S. Bank branch location in Walmart located at 103<sup>rd</sup> and Silver Spring in Milwaukee, WI, in the name of A.G. The entire transaction was videotaped. An unidentified African American male entered the US Bank office area Williams managed. Williams appears to enter information into the US Bank computer without any input from the unidentified subject. No paperwork or identification was ever produced by the unidentified subject during the course of the account opening. Furthermore, while the account was in the name of A.G., the social security number of R.S. was used to open the account.

At approximately 12:04pm, the unidentified subject provided a signature on an electronic signature pad. According to US Bank records, Williams opened the A.G. account, and signature cards on the A.G. accounts were created at the same time the unidentified male signed the electronic signature pad. The unidentified subject then left the US Bank offices. US Bank records reflect that a checking account, line of credit, two credit cards, and three debit cards were thereafter opened and subsequently issued in the name of A.G. Later that same day, an unidentified female made a \$25 opening deposit into the account. Williams accepted the deposit. The mailing address associated with the account to receive the debit card, credit card, and bank statements was 2917 S. Claire Blvd in Robbins, IL. According to NCIC printouts, this address was commonly used by Anthony Sykes. Several notable transactions were made to the account in the name of A.G. as detailed below.

12. On August 16, 2013, there is a Neiman Marcus charge for \$677.35 for a knit shirt in the amount of \$295, and a belt in the amount of \$325, made to the A.G. credit card. Consistent with the above Neiman Marcus charge, on August 20, 2013, a photograph was posted on the Anthony Sykes Facebook page showing a Gucci knit shirt and a Gucci Belt.

13. On August 18, 2013, there is a Amtrak charge made on the A.G. credit card for a ticket to Washington, DC in the amount of \$174. On the same day, a post on the Anthony Sykes Facebook page reflects the following: "I jus paid \$175 for a train ticket smh."

14. On September 3, 2013, Williams fraudulently opened two accounts using the identities of R.P. and F.K. at the US Bank branch inside Walmart on 103rd and W. Silver Spring Drive in Milwaukee, WI. The entire transaction was videotaped. Anthony Sykes and Deandre Miller, both African American males in their early twenties, entered the US Bank office area and sat across from Williams as he entered information on a computer. There was almost no

interaction between Williams and the two subjects during the account opening. No paper forms were filled out or provided to Williams and neither Sykes or Miller ever produced any identification to Williams during that meeting. Miller and Sykes, however, were obviously not R.P. and F.K. as these subjects were 68 and 79 years old, respectively, at the time of the account opening.

15. Miller provided e-signatures to open the R.P. accounts. At approximately 6:15 p.m., and again at 6:19 p.m., Miller provided an e-signature on an electronic signature pad. According to US Bank records, signature cards for two accounts were created for R.P. at the above times and the accounts opened included a checking account, and a money market savings account. A credit card and two debit cards were issued for the account. Account statements were subsequently mailed to 1900 Broadway Street, Apt. 1B, Blue Island, IL. The real R.P. resides in Arizona.

16. Sykes provided e-signatures to open the F.K. accounts. At approximately 6:23pm and again at 6:28 pm, Sykes provided signatures on an electronic signature pad. According to US Bank records, signature cards for two accounts were created for F.K. at the above times and the accounts opened included a checking account, and a money market savings account. A credit card and two debit cards were issued for the account. Account statements were subsequently mailed to 2940 139th Place in Blue Island, IL. According to NCIC printouts, Deandre Miller has frequently used this mailing address in the past. Furthermore, a phone number listing to Miller was used to activate the credit card account.

17. After both accounts were opened, Sykes and Miller provided cash to Williams, presumably for opening deposits on the accounts. The two men then left the bank. Thereafter, from September 17 to November 3, 2013, numerous credit card and debit card transactions were



made on the R.P. account. The transactions occurred in Illinois, including Blue Island, IL, and Robbins, IL, an area where both Sykes and Miller originate; transactions also occurred in Annapolis, MD. Several Facebook posts indicative of the subjects fraudulent purchases under the R.P. account are detailed below.

18. On September 16, 2013, a video was posted to the timeline on the Anthony Sykes Facebook. The video appeared to show Sykes shopping for athletic shoes at a shopping mall in Baltimore, MD.

19. On September 17, 2013, there is a charge from American Airlines on the R.P. credit card for an airline ticket in the name of Anthony Sykes for a flight from Baltimore to Chicago O'Hare on September 20, 2013. Notably, from September 17, 2013, through September 20, 2013, several charges were made on the R.P. credit card in and around Baltimore, MD. These charges included purchases from several retail stores such as the Dr. Denim, Michael Kors, Champs, and Sunglass Hut, all located in Annapolis, MD. Annapolis, MD is approximately 30 miles from Baltimore, MD.

20. On September 20, 2013, a photograph of an American Airlines plane on the runway was posted on the Anthony Sykes Facebook page which stated the following: "Fresh off the Jet to the Set where my G's at! Im back home...Now Lets Mf Get It!" Notably, the flight fraudulently purchased on the R.P. credit card in the name of Anthony Sykes as discussed above was scheduled to land in Chicago, IL, on the same date this message and photograph were posted.

21. On September 21, 2013, there are photographs and postings with the caption ".....its gone b a ZOO in #BBL 2night" and "Dirty Money for the watch...But its so CLEAN! I hope the bottle girls got enuff sparkles! Ima make that bitch light up! #bandzhoe #dmg #layh #600 #billboardlive #epic," posted on the timeline of the Anthony Sykes Facebook page. Based on my



investigation, "BBL" is short for Billboard Live, a sports bar located in Markham, IL, a suburb of south Chicago. On September 22, 2013, there is a charge from Billboard Live in the amount of \$1,125.00 charged to the R.P. credit card.

22. On September 29, 2013, a picture of a plate of food and a caption that indicated he was at the Island Sports Bar was posted on the Anthony Sykes Facebook page. Consistent with the Facebook post, the R.P. credit card statement reflects that on the same date, a purchase totaling \$38.83 was made at the Island Sports Bar in Blue Island, IL.

23. Similarly, on October 6, 2013, there is a photograph of a receipt from the Island Sports Bar with food charges in the amount of \$71.96 posted on the Facebook page for Anthony Sykes. Consistent with the Facebook post, the R.P. credit card statement reflects that on the same date, a purchase totaling \$71.96 was made at the Island Sports Bar.

24. On October 21, 2013, U.S. Bank Corporate Security was notified by U.S. Bank Employee Fraud Detection of Identity Theft involving three separate U.S. Bank accounts. The three accounts under investigation were all opened by U.S. Bank In-Store Assistant Manager Edward Anthony Williams.

25. On October 22, 2013, U.S. Bank Corporate Security Senior Fraud Investigators interviewed Edward Anthony Williams. Williams told investigators that he received personal identity information of three to four subjects via text message from a person later identified as Anthony Sykes. Williams said he subsequently opened checking, savings, line of credit, and credit card accounts in the victim's names. Williams stated he received \$1,800 cash as payment for opening the fraudulent accounts. Williams was terminated from U.S. Bank.

26. On October 25, 2013, and November 3, 2013, victims F.K. and R.P., notified U.S. Bank that their personal identity information was stolen and that they did not open any accounts

with U.S. Bank.

### **Facebook Searches**

27. I conducted searches in social media including Facebook for Anthony Sykes, and Deandre Miller. I determined from photographs and other information that the Facebook account names for the suspects in the above crime were as follows:

- a. Anthony Sykes:  
Facebook Name: "Anthony Sykes" or "Anthony.y.sykes"  
Facebook ID 506758797
- b. Deandre Miller:  
Facebook Name: "Deandre Miller"  
Facebook ID: 511640886

28. A review of the Facebook account for "Anthony Sykes" showed numerous transactions that implicated the use of the victim credit cards as detailed in the above paragraphs.

29. A review of the Facebook account for "Deandre Miller" revealed that Sykes and Miller were Facebook friends during the offense conduct and remain Facebook friends today. Photographs posted on the Deandre Miller Facebook account during the offense conduct include announcements of events featuring Anthony Sykes at Billboard Live, a night club in Markham, IL. Additionally, during the offense conduct, several charges from Billboard Live, a night club located in Markham, IL, were made to the victim credit cards.

30. I have requested Facebook preserve the above-listed accounts during the time frame the offenses were committed in 2013.

31. Facebook owns and operates a free-access social networking website of the same name that can be accessed at <http://www.facebook.com>. Facebook allows its users to establish accounts with Facebook, and users can then use their accounts to share written news, photographs, videos, and other information with other Facebook users, and sometimes with the general public.

32. Facebook asks users to provide basic contact and personal identifying information to Facebook, either during the registration process or thereafter. This information may include the user's full name, birth date, gender, contact e-mail addresses, Facebook passwords, Facebook security questions and answers (for password retrieval), physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers. Facebook also assigns a user identification number to each account.

33. Facebook users may join one or more groups or networks to connect and interact with other users who are members of the same group or network. Facebook assigns a group identification number to each group. A Facebook user can also connect directly with individual Facebook users by sending each user a "Friend Request." If the recipient of a "Friend Request" accepts the request, then the two users will become "Friends" for purposes of Facebook and can exchange communications or view information about each other. Each Facebook user's account includes a list of that user's "Friends" and a "News Feed," which highlights information about the user's "Friends," such as profile changes, upcoming events, and birthdays.

34. Facebook users can select different levels of privacy for the communications and information associated with their Facebook accounts. By adjusting these privacy settings, a Facebook user can make information available only to himself or herself, to particular Facebook users, or to anyone with access to the Internet, including people who are not Facebook users. A Facebook user can also create "lists" of Facebook friends to facilitate the application of these privacy settings. Facebook accounts also include other account settings that users can adjust to control, for example, the types of notifications they receive from Facebook.

35. Facebook users can create profiles that include photographs, lists of personal interests, and other information. Facebook users can also post "status" updates about their

whereabouts and actions, as well as links to videos, photographs, articles, and other items available elsewhere on the Internet. Facebook users can also post information about upcoming “events,” such as social occasions, by listing the event’s time, location, host, and guest list. In addition, Facebook users can “check in” to particular locations or add their geographic locations to their Facebook posts, thereby revealing their geographic locations at particular dates and times. A particular user’s profile page also includes a “Wall,” which is a space where the user and his or her “Friends” can post messages, attachments, and links that will typically be visible to anyone who can view the user’s profile.

36. Facebook allows users to upload photos and videos, which may include any metadata such as location that the user transmitted when s/he uploaded the photo or video. It also provides users the ability to “tag” (i.e., label) other Facebook users in a photo or video. When a user is tagged in a photo or video, he or she receives a notification of the tag and a link to see the photo or video. For Facebook’s purposes, the photos and videos associated with a user’s account will include all photos and videos uploaded by that user that have not been deleted, as well as all photos and videos uploaded by any user that have that user tagged in them.

37. Facebook users can exchange private messages on Facebook with other users. These messages, which are similar to e-mail messages, are sent to the recipient’s “Inbox” on Facebook, which also stores copies of messages sent by the recipient, as well as other information. Facebook users can also post comments on the Facebook profiles of other users or on their own profiles; such comments are typically associated with a specific posting or item on the profile. In addition, Facebook has a Chat feature that allows users to send and receive instant messages through Facebook. These chat communications are stored in the chat history for the account.

Facebook also has a Video Calling feature, and although Facebook does not record the calls themselves, it does keep records of the date of each call.

38. If a Facebook user does not want to interact with another user on Facebook, the first user can “block” the second user from seeing his or her account.

39. Facebook has a “like” feature that allows users to give positive feedback or connect to particular pages. Facebook users can “like” Facebook posts or updates, as well as webpages or content on third-party (i.e., non-Facebook) websites. Facebook users can also become “fans” of particular Facebook pages.

40. Facebook has a search function that enables its users to search Facebook for keywords, usernames, or pages, among other things.

41. Each Facebook account has an activity log, which is a list of the user’s posts and other Facebook activities from the inception of the account to the present. The activity log includes stories and photos that the user has been tagged in, as well as connections made through the account, such as “liking” a Facebook page or adding someone as a friend. The activity log is visible to the user but cannot be viewed by people who visit the user’s Facebook page.

42. Facebook Notes is a blogging feature available to Facebook users, and it enables users to write and post notes or personal web logs (“blogs”), or to import their blogs from other services, such as Xanga, LiveJournal, and Blogger.

43. The Facebook Gifts feature allows users to send virtual “gifts” to their friends that appear as icons on the recipient’s profile page. Gifts cost money to purchase, and a personalized message can be attached to each gift. Facebook users can also send each other “pokes,” which are free and simply result in a notification to the recipient that he or she has been “poked” by the sender.

44. Facebook also has a Marketplace feature, which allows users to post free classified ads. Users can post items for sale, housing, jobs, and other items on the Marketplace.

45. In addition to the applications described above, Facebook also provides its users with access to thousands of other applications (“apps”) on the Facebook platform. When a Facebook user accesses or uses one of these applications, an update about that the user’s access or use of that application may appear on the user’s profile page.

46. Some Facebook pages are affiliated with groups of users, rather than one individual user. Membership in the group is monitored and regulated by the administrator or head of the group, who can invite new members and reject or accept requests by users to enter. Facebook can identify all users who are currently registered to a particular group and can identify the administrator and/or creator of the group. Facebook uses the term “Group Contact Info” to describe the contact information for the group’s creator and/or administrator, as well as a PDF of the current status of the group profile page.

47. Facebook uses the term “Neoprint” to describe an expanded view of a given user profile. The “Neoprint” for a given user can include the following information from the user’s profile: profile contact information; News Feed information; status updates; links to videos, photographs, articles, and other items; Notes; Wall postings; friend lists, including the friends’ Facebook user identification numbers; groups and networks of which the user is a member, including the groups’ Facebook group identification numbers; future and past event postings; rejected “Friend” requests; comments; gifts; pokes; tags; and information about the user’s access and use of Facebook applications.

48. Facebook also retains Internet Protocol (“IP”) logs for a given user ID or IP address. These logs may contain information about the actions taken by the user ID or IP address on



Facebook, including information about the type of action, the date and time of the action, and the user ID and IP address associated with the action. For example, if a user views a Facebook profile, that user's IP log would reflect the fact that the user viewed the profile, and would show when and from what IP address the user did so.

49. Social networking providers like Facebook typically retain additional information about their users' accounts, such as information about the length of service (including start date), the types of service utilized, and the means and source of any payments associated with the service (including any credit card or bank account number). In some cases, Facebook users may communicate directly with Facebook about issues relating to their accounts, such as technical problems, billing inquiries, or complaints from other users. Social networking providers like Facebook typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications.

50. As explained herein, information stored in connection with a Facebook account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, a Facebook user's "Neoprint," IP log, stored electronic communications, and other data retained by Facebook, can indicate who has used or controlled the Facebook account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, profile contact information, private messaging logs, status updates, and tagged photos (and the data associated with the foregoing, such as date and time) may be evidence of who used or controlled the Facebook account at a relevant time. Further, Facebook



account activity can show how and when the account was accessed or used. For example, as described herein, Facebook logs the Internet Protocol (IP) addresses from which users access their accounts along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the account access and use relating to the crime under investigation. Such information allows investigators to understand the geographic and chronological context of Facebook access, use, and events relating to the crime under investigation. Additionally, Facebook builds geo-location into some of its services. Geo-location allows, for example, users to “tag” their location in posts and Facebook “friends” to locate each other. This geographic and timeline information may tend to either inculcate or exculpate the Facebook account owner. Last, Facebook account activity may provide relevant insight into the Facebook account owner’s state of mind as it relates to the offense under investigation. For example, information on the Facebook account may indicate the owner’s motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

51. Therefore, the computers of Facebook are likely to contain all the material described above, including stored electronic communications and information concerning subscribers and their use of Facebook, such as account access information, transaction information, and other account information.

#### **INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED**

52. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Facebook to disclose to the government copies of the records and other information

(including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

#### **IV. CONCLUSION**

53. Based on a review of the subjects' messages and photographs posted on Facebook, I believe that obtaining complete records from their Facebook accounts will reveal phone numbers and IP addresses associated with the suspects, location of the suspects during the fraud activity, and communication between the suspects regarding the criminal activity described herein.

#### **REQUEST FOR SEALING**

54. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. A formal motion will be submitted by the government upon the return of this warrant. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of

the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may jeopardize the investigation.

## ATTACHMENT A

### Facebook Accounts to be Searched

| NAME           | FACEBOOK IDENTIFICATION (UID) | FACEBOOK NAME                       |
|----------------|-------------------------------|-------------------------------------|
| Anthony Sykes  | 506758797                     | Anthony Sykes or Anthony.y.sykes    |
| Deandre Miller | 511640886                     | Deandre Miller or Deandremiller1987 |

## **ATTACHMENT B**

### **Particular Things to be Seized**

#### **I. Information to be disclosed by Facebook**

To the extent that the information described in Attachment A is within the possession, custody, or control of Facebook Inc. ("Facebook"), including any messages, records, files, logs, or information that have been deleted but are still available to Facebook, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Facebook is required to disclose the following information to the government for each user ID listed in Attachment A:

- (a) All contact and personal identifying information, including for user IDs 506758797, 511640886: full name, user identification number, birth date, gender, contact e-mail addresses, Facebook passwords, Facebook security questions and answers, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers.
- (b) All activity logs for the account and all other documents showing the user's posts and other Facebook activities;
- (c) All photos and videos uploaded by that user ID and all photos and videos uploaded by any user that have that user tagged in them;
- (d) All profile information; News Feed information; status updates; links to videos, photographs, articles, and other items; Notes; Wall postings; friend lists, including the friends' Facebook user identification numbers; groups and networks of which the user is a member, including the groups' Facebook group identification numbers; future and past event postings; rejected "Friend" requests; comments; gifts; pokes; tags; and information about the user's access and use of Facebook applications;
- (e) All other records of communications and messages made or received by the user, including all private messages, chat history, video calling history, and pending "Friend" requests;

- (f) All "check ins" and other location information;
- (g) All IP logs, including all records of the IP addresses that logged into the account;
- (h) All records of the account's usage of the "Like" feature, including all Facebook posts and all non-Facebook webpages and content that the user has "liked";
- (i) All information about the Facebook pages that the account is or was a "fan" of;
- (j) All past and present lists of friends created by the account;
- (k) All records of Facebook searches performed by the account;
- (l) All information about the user's access and use of Facebook Marketplace;
- (m) The types of service utilized by the user;
- (n) The length of service (including start date) and the means and source of any payments associated with the service (including any credit card or bank account number);
- (o) All privacy settings and other account settings, including privacy settings for individual Facebook posts and activities, and all records showing which Facebook users have been blocked by the account;
- (p) All records pertaining to communications between Facebook and any person regarding the user or the user's Facebook account, including contacts with support services and records of actions taken

## **II. Information to be seized by the government**

All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of Title 18 U.S. Code § 1344 – Bank Fraud and 18 U.S. Code § 1028A - Aggravated identity theft involving Anthony Sykes, and Deandre Miller between the dates of July 1, 2013 to November 1, 2013, including, for each user ID identified on Attachment A, information pertaining to the following matters:

- (a) Communications between known subjects. Communications between known subjects and unknown subjects. Photographs and video of evidence or proceeds of the fraud. Preparatory steps taken in furtherance of the fraud.

- (b) Evidence indicating how and when the Facebook account was accessed or used, to determine the chronological and geographic context of account access, use, and events relating to the crime under investigation and to the Facebook account owner;
- (c) Evidence indicating the Facebook account owner's state of mind as it relates to the crime under investigation;
- (d) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).
- (e) Communications related to photos/attachments relevant to the crime.
- (f) Communications related to travel relevant to the crime.
- (g) Communications related to dates relevant to the crime.